(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 091 275 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
11.04.2001 Bulletin 2001/15

(51) Int. Cl.[7]: **G06F 1/00**

(21) Application number: **00308721.0**

(22) Date of filing: **04.10.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **04.10.1999 US 411665**

(71) Applicant:
CANON KABUSHIKI KAISHA
Tokyo (JP)

(72) Inventors:
- **Mazzagatte, Craig,**
  c/o Canon Information Syst. Inc
  Irvine, California 92612 (US)
- **Slick, Royce E.,**
  c/o Canon Information Syst. Inc.
  Irvine, California 92612 (US)
- **Iwamoto, Neil,**
  c/o Canon Information Systems Inc.
  Irvine, California 92612 (US)

(74) Representative:
Beresford, Keith Denis Lewis et al
BERESFORD & Co.
High Holborn
2-5 Warwick Court
London WC1R 5DJ (GB)

(54) Authenticated secure printing

(57) Authorized printout of an image corresponding to print data received at a print node from a network. The authorized printout comprises encrypting print data by a print node and storing the encrypted print data without printout, receiving authentication of an intended recipient to print the print data, and decrypting the encrypted print data by the print node and printing the decrypted print data by an image forming device, responsive to receipt of authentication in the receiving step. The print node may be the image forming device itself or a gateway to multiple image forming devices. The print node encrypts the print data with either a symmetric key or an asymmetric key.

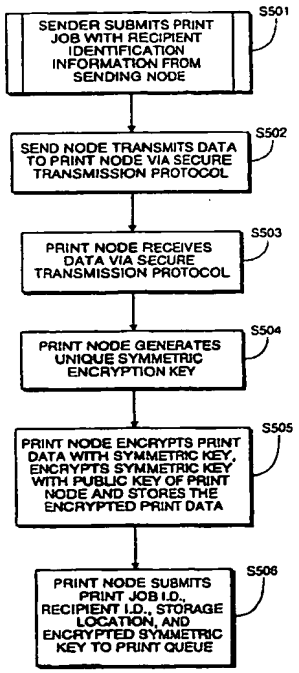

FIG. 5

EP 1 091 275 A2

Description

[0001] The present invention concerns authorized printing wherein a hard-copy image is printed only in the presence of an intended recipient. In particular, the invention concerns encryption of print data by a print node, and storing the encrypted print data without printout until the print node receives proper authentication from the intended recipient.

[0002] In a network environment, a print job generated at one location in the network can be printed at another location. Occasionally, confidential or otherwise sensitive information has to be printed. When the confidential information is transmitted to the printer, the sender may want to protect the data transmission over the network from electronic interception or at least prevent unauthorized viewing of the hard-copy printout. Generally, common encryption protocols such as SSL or TLS can be used to provide the required security from electronic interception of the transmission. Nonetheless, concerns remain about unauthorized viewing of the hard-copy printed output or electronic viewing of print jobs stored in the print queue.

[0003] In particular, if a print job containing confidential information is sent to a printer, the sender may not be present at the printer when the image is printed. During the time that it takes the sender to reach the printer to pick-up the hard-copy print job, the printed output can be viewed by any person who comes across the printed output before the sender has reached the printer. As a result, confidential information may be compromised by being viewed by an unauthorized person.

[0004] In addition, if the sender reaches the printer before the printer prints the image, and numerous print jobs are pending in the print queue before his, the sender would have to wait until all previously pending print jobs are printed before he can obtain his print job. As a result, the sender must either spend time waiting for his print job to print out or return later. In the latter case, the sender risks the possibility that his confidential print out will be printed before he is able to return.

[0005] Further, print jobs that have been stored in a file (local to the printer or in a remote file server) prior to printout are subject to electronic viewing by unauthorized personnel. Therefore, the stored print data must also be protected from unauthorized viewing.

[0006] Similar issues arise with a facsimile transmission. Namely, the printed output can be viewed by any person who arrives at the destination facsimile machine before the intended recipient.

[0007] Therefore, a method of printing an image only in the presence of the intended recipient and securely storing print data is needed.

[0008] One method of printing a document only in the presence of the intended recipient is disclosed in U.S. Patent No. 5,633,932. According to the patent, a sending node encrypts a print job and a printing node decrypts the print job prior to printout. If the print job contains confidential information, the sending node generates an encrypted header signifying that fact, using a public key of the printing node. The printing node contains its own private key, and upon receiving the encrypted print job, decrypts the header to ascertain whether the document requires authentication by the intended recipient before printing. If so, the print data is stored without printout in encrypted form until the print node receives the proper authentication from the intended recipient. If the print node determines that the document does not require authentication, the print node decrypts and prints the document.

[0009] The present invention also ensures that printout of sensitive documents is authorized and that the print data is securely stored, but it does so in ways that are different from the aforementioned U.S. Patent No. 5,633,932.

[0010] The present invention achieves authorized printout of print data received by a print node by encrypting the print data at the print node and storing the encrypted print data without printout until the print node receives authentication from the intended recipient. Once the proper authentication is presented, the print node decrypts the print data and a printout is generated by the print node based on the print data.

[0011] Accordingly, in one aspect the invention is authorized printout of an image corresponding to print data received at a print node from a network. The print data is encrypted by the print node and the encrypted print data is stored without printout. The print node then receives authentication from the intended recipient to print the print data. In response to the authentication, the print node decrypts the encrypted print data and the image is printed by an image forming device.

[0012] As a result of the foregoing arrangement, a print job having confidential information can only be printed in the presence of the intended recipient having the proper authentication. Also, the print data sent to the print node is securely stored by being encrypted by the print node, which uses a key unique to the print node such that the encrypted print data can only be decrypted by the print node after the intended recipient has supplied proper authentication to the print node.

[0013] Additionally, the print job is not required to be encrypted at the sending node before being sent to the print node. However, in order to provide secure data transmission over the network, a secure data transmission protocol, such as SSL (Secure Sockets Layer) or TLS (Transport Layer Security) can be used to provide a more efficient transmission from the sending node to the print node.

[0014] In further aspects of the foregoing arrangement, the print node may be any image forming device, such as a printer or a facsimile, connectable to a network and having the capability of performing the print data encryption/decryption itself. Alternatively, the print node may be a gateway connected to multiple printers,

where the gateway performs the print data encryption/decryption.

[0015] Also, smart-cards or smart-card chips are preferably utilized to supply the authentication to the print node. The smart-cards are preferably read by a smart-card reader located at the image forming device and connected to the print node so that the print node can confirm that the intended recipient is present at the image forming device when the image is printed.

[0016] Additionally, the encryption performed by the print node may be performed using either a symmetric algorithm or an asymmetric (public/private key) algorithm. As further security, a symmetric key may be further encrypted by an asymmetric key.

[0017] This brief summary has been provided so that the nature of the invention may be understood quickly. A more complete understanding of the invention can be obtained by reference to the following detailed description of the preferred embodiments of the invention, which are described by way of example only, with reference to the attached drawings in which:

Figure 1 is a representative view of a networked computing environment in which an embodiment of the present invention may be implemented.

Figure 2 is a detailed block diagram showing the internal architecture of the computer shown in Figure 1 according to an embodiment of the present invention.

Figure 3 is a detailed block diagram showing the internal architecture of the printer shown in Figure 1 according to an embodiment of the present invention.

Figure 4 is a detailed block diagram showing the server shown in Figure 1 according to an embodiment of the present invention.

Figure 5 is a flowchart depicting a print node encrypting print data and storing the encrypted print data according to an embodiment of the present invention.

Figure 6 is a flowchart depicting a print node decrypting encrypted print data and printing an image based on the decrypted print data where the print node is an image forming device itself.

Figure 7A is a flowchart depicting a print node transmitting encrypted print data and a symmetric key to an image forming device via a secure transmission protocol where the print node is a gateway to multiple image forming devices.

Figure 7B is a flowchart depicting a print node decrypting encrypted print data and transmitting the decrypted print data to an image forming device via a secure transmission protocol where the print node is a gateway to multiple image forming devices.

Figure 8 is a flowchart depicting a print node transmitting an encrypted symmetric key and encrypted print data to an image forming device via a non-secure transmission protocol where the print node is a gateway to multiple image forming devices.

[0018] The present invention is generally directed to secure printing of image data such that the image data can only be printed on an image forming device in the presence of an intended recipient. The present invention therefore provides a manner by which a document can be securely transmitted from a computer to a remote image forming device in a networked environment, such as a Local Area Network (LAN), a Wide Area Network (WAN), or the Internet. The document is maintained in a secure fashion until the intended recipient is present at the image forming device, whereupon the image forming device prints the image.

[0019] Figure 1 provides an overall system view of a networked computing environment in which an embodiment of the present invention may be implemented. As shown in Figure 1, the networked computing environment comprises a network which is connected to desktop computer 10, laptop computer 20, server 40, digital copier 30 and printer 50. Network 100 is preferably an Ethernet network medium consisting of a bus-type physical architecture, although the invention can be utilized over other types of networks, including the Internet.

[0020] Desktop computer 10 is preferably an IBM PC-compatible computer having a windowing environment such as Microsoft Windows 95, Windows 98 or Windows NT. As is typical with IBM PC-compatible computers, desktop computer 10 preferably has a display, keyboard, mouse, floppy drive and/or other type of storage medium (not shown). Also attached to desktop computer 10 is smart-card interface device 15 for interfacing with a smart-card of a computer user, such as smart-card 16. Smart-card 16 therefore provides a mechanism whereby a computer user can authenticate the user's identity to desktop computer 10. In addition, smart-card 16 contains a private key of a private/public key pair which is specific to a computer user and which is used in the present invention for the secure printing of image data as discussed more fully below.

[0021] Laptop computer 20 is also an IBM PC-compatible computer having a windowing environment such as Microsoft Windows 95, Windows 98 or Windows NT. Like desktop computer 10, laptop computer 20 also has a display, keyboard, mouse and floppy drive or other storage means (not shown). In addition, laptop computer 20 also has a smart-card interface device 25 attached to it for interfacing to the smart-card of a computer user such as smart-card 26. Also attached to network 100 is digital copier 30, which is capable of receiving image data over network 100 for printing. Digital copier 30 also has attached smart-card interface device 35 for interfacing with the smart-card of a print job recipient, such as smart-card 36. In addition, server 40 is also connected to network 100. Server 40 preferably comprises an IBM PC-compatible computer having

an operating system such as DOS, Microsoft Windows 95, Windows 98 or Windows NT, UNIX or other operating system. Server 40 has a storage device 41 which is preferably a large fixed disk for storing numerous files. Server 40 can therefore be utilized by other devices on network 100 as a file server and may also act as a gateway for other devices on network 100 to another network such as the Internet.

[0022] Printer 50 is also connected to network 100 and is preferably a laser or bubble-jet printer which is capable of operating as both a printer and a facsimile device. Printer 50 has a storage device 51 which is preferably a large fixed disk, and also has an embedded smart-chip 57 which contains a private key of a private/public key pair corresponding to printer 50 for use in encryption and/or decryption of data received by printer 50. In addition, printer 50 is connected to smart-card interface device 55 which is capable of interfacing with a smart-card of a print job recipient, such as smart-card 56. In this manner, the printing of a print job for a particular intended recipient may be controlled through the use of smart-card interface device 55 and smart-card 56, in combination with smart-chip 57 in printer 50.

[0023] Figure 2 is a block diagram showing an overview of the internal architecture of desktop computer 10. In Figure 2, desktop computer 10 is seen to include central processing unit (CPU) 210 such as a programmable microprocessor which is interfaced to computer bus 200. Also coupled to computer bus 200 are keyboard interface 220 for interfacing to a keyboard, mouse interface 230 for interfacing to a pointing device, floppy disk interface 240 for interfacing to a floppy disk, display interface 250 for interfacing to a display, network interface 260 for interfacing to network 100, and smart-card interface 265 for interfacing to smart-card interface device 15.

[0024] Random access memory ("RAM") 270 interfaces to computer bus 200 to provide central processing unit ("CPU") 210 with access to memory storage, thereby acting as the main run-time memory for CPU 210. In particular, when executing stored program instruction sequences, CPU 210 loads those instruction sequences from fixed disk 280 (or other memory media) into random access memory ("RAM") 270 and executes those stored program instruction sequences out of RAM 270. It should also be noted that standard-disk swapping techniques available under windowing operating systems allow segments of memory to be swapped to and from RAM 270 and fixed disk 280. Read-only memory ("ROM") 290 stores invariant instruction sequences, such as start-up instruction sequences for CPU 210 or basic input/output operation system ("BIOS") sequences for the operation of peripheral devices attached to computer 10.

[0025] Fixed disk 280 is one example of a computer-readable medium that stores program instruction sequences executable by central processing unit ("CPU") 210 so as to constitute operating system 281, printer driver 282, smart-card interface driver 283, other drivers 284, word processing program 285, other programs 286, e-mail program 287 and other files 288. As mentioned above, operating system 281 is preferably a windowing operating system, although other types of operating systems may be used with the present invention. Printer driver 282 is utilized to prepare image data for printing on at least one image forming device, such as printer 50. Smart-card interface driver 283 is utilized to drive and control smart-card interface 265 for interfacing with smart-card interface device 15 so as to read and write to a smart-card such as smart-card 16. Other drivers 284 include drivers for each of the remaining interfaces which are coupled to computer bus 200.

[0026] Word processing program 285 is a typical word processor program for creating documents and images, such as Microsoft Word, or Corel WordPerfect. Other programs 286 contains other programs necessary to operate desktop computer 10 and to run desired applications. E-mail program 287 is a typical e-mail program that allows desktop computer 10 to receive and send e-mails over network 100. Other files 288 include any of the files necessary for the operation of desktop computer 10 or files created and/or maintained by other application programs on desktop computer 10.

[0027] Figure 3 is a block diagram showing an overview of the internal architecture of printer 50. In Figure 3, printer 50 is seen to contain a printer smart-chip 57 which, as previously mentioned, contains a private key corresponding to printer 50 for encryption/decryption purposes. Printer 50 also contains a central processing unit ("CPU") 310 such as a programmable microprocessor which is interfaced to printer bus 300. Also coupled to printer bus 300 are control logic 320, which is utilized to control the printer engine of printer 50 (not shown), I/O ports 330 which is used to communicate with various input/output devices of printer 50 (not shown), smart-card interface 365 which is utilized to interface with smart-card interface device 55, and network interface 360 which is utilized to interface printer 50 to network 100.

[0028] Also coupled to printer bus 300 are EEPROM 340, for containing non-volatile program instructions, random access memory ("RAM") 370, printer memory 51 and read-only memory ("ROM") 390. RAM 370 interfaces to printer bus 300 to provide CPU 310 with access to memory storage, thereby acting as the main run-time memory for CPU 310. In particular, when executing stored program instruction sequences, CPU 310 loads those instruction sequences from printer memory 51 (or other memory media) into RAM 370 and executes those stored program instruction sequences out of RAM 370. ROM 390 stores invariant instruction sequences, such as start-up instruction sequences for CPU 310 or BIOS sequences for the operation of various peripheral devices of printer 50 (not shown).

[0029] Printer memory 51 is one example of a computer-readable medium that stores program instruction

sequences executable by CPU 310 so as to constitute printer engine logic 351, control logic driver 352, I/O port drivers 353, smart-card interface driver 354, encryption/decryption logic 355, queue 356, other files 357, printer smart-chip driver 358, and e-mail program 359. Printer engine logic 351 and control logic driver 352 are utilized to control and drive the printer engine of printer 50 (not shown) so as to print an image according to image data received by printer 50, preferably over network 100. I/O port drivers 353 are utilized to drive the input and output devices (not shown) connected through I/O ports 330. Smart-card interface driver 354 is utilized to drive smart-card interface 365 for interfacing to smart-card interface device 55, thereby enabling printer 50 to read and write to a smart-card such as smart-card 56.

[0030] Encryption/decryption logic 355 enables printer 50 to receive encrypted data according to the present invention and to carry out the necessary steps to enable the decryption of the encrypted print data in the presence of an intended recipient. The details of these steps are discussed more fully below. Queue 356 is utilized to contain a print queue comprised of numerous print jobs which are to be printed. Other files 357 contain other files and/or programs for the operation of printer 50. Printer smart-chip driver 358 is utilized to interface with printer smart-chip 57 for certain cryptographic operations. Lastly, e-mail program 359 is a typical e-mail program for enabling printer 50 to receive e-mail messages from network 100. Such e-mail messages may contain print job-related information, as discussed in more detail below.

[0031] Figure 4 is a block diagram showing an overview of the internal architecture of server 40. In Figure 4, server 40 is seen to include a central processing unit ("CPU") 410 such as a programmable microprocessor which is interfaced to computer bus 400. Also coupled to computer bus 400 is a network interface 460 for interfacing to network 100. In addition, random access memory ("RAM") 470, fixed disk 41, and read-only ("ROM") 490 are also coupled to computer bus 400. RAM 470 interfaces to computer bus 400 to provide CPU 410 with access to memory storage, thereby acting as the main run-time memory for CPU 410. In particular, when executing stored program instruction sequences, CPU 410 loads those instruction sequences from fixed disk 41 (or other memory media) into RAM 470 and executes those stored program instruction sequences out of RAM 470. It should also be recognized that standard disk-swapping techniques allow segments of memory to be swapped to and from RAM 470 and fixed disk 41. ROM 490 stores invariant instruction sequences, such as start-up instruction sequences for CPU 410 or basic input/output operating system ("BIOS") sequences for the operation of peripheral devices which may be attached to server 40 (not shown).

[0032] Fixed disk 41 is one example of a computer-readable medium that stores program instruction sequences executable by CPU 410 so as to constitute operating system 411, network interface driver 412, encryption/decryption logic 413, e-mail program 414, queue 415, and other files 416. As mentioned above, operating system 411 can be an operating system such as DOS, Windows 95, Windows 98, Windows NT, UNIX, or other such operating system. Network interface driver 412 is utilized to drive network interface 460 for interfacing server 40 to network 100. Encryption/decryption logic 413 allows server 40 to receive encrypted data and to either maintain such data in queue 415 or to send such data to an image forming device such as printer 50 for printing. Encyrption/decryption logic 413 is generally only required where a secure transmission protocol is used between the server and the printer. E-mail program 414 is a typical e-mail program and enables server 40 to receive and/or send e-mail messages over network 100. Queue 415 is utilized to store numerous print jobs for output on one or more image forming devices, such as printer 50. Lastly, other files 416 contains other files or programs necessary to operate server 40 and/or to provide additional functionality to server 40.

[0033] Authenticated secure printing according to the present invention will now be described in more detail with regard to Figures 5 through 8.

[0034] It should be noted that with regard to the terms "sender" and "intended recipient" as used in the following discussion, "sender" refers to the person who submits a print job from the host computer to be printed out by an image forming device. The "intended recipient" refers to the person who arrives at the image forming device to retrieve the print job. In some cases, the sender and the intended recipient may be one in the same. That is, the person who sends the print job may intend that he/she be the only person to retrieve the printout from the image forming device. In other cases, the sender and the intended recipient may be different individuals. For example, the sender may submit a print job that he intends only to be retrieved by a specified person other than him/herself. However, for the purposes of the following discussion, the term "sender/intended recipient" refers to the person holding the proper authentication information to retrieve the image from the image forming device.

[0035] Additionally, the term "image forming device" as it relates to the following discussion means a printer, such as a laser-jet or ink-jet printer. However, it should be noted that the present invention may be utilized in any image forming device, such as a facsimile, or a remote computer having a display.

[0036] Referring now to the drawings, Figure 5 is a flowchart depicting a print job being submitted to a print node, the print node encrypting the print data and storing the encrypted print data according to the present invention.

[0037] In this regard, the term "print node" means either an image forming device or a gateway to one or multiple image forming devices. That is, the print node

may be an image forming device itself provided with the capability of performing encryption/decryption tasks, or the print node may be a gateway, such as a network server, that provides the capability of performing the encryption/decryption tasks.

[0038] As seen in Figure 5, in step S501 the sender submits a print job from a sending node, such as desktop computer 10 or laptop computer 20. The print job is generally submitted through commonly known printer driver techniques. For example, if the sender is utilizing a word processor application program, such as Microsoft Word or Corel Wordperfect, and wants to print the document, he would normally select a print option within the application program, thereby activating a printer driver. The printer driver usually permits the sender to select printing options, such as printing speed, print resolution, or number of copies.

[0039] One such print option is an option to select a secure or non-secure transmission mode, whereby a printer driver selects either a secure or non-secure transmission protocol for transmitting the print job based on the senders selection. For example, the sender may opt for a normal (non-secure) transmission mode, in which case the print driver transmits the print job over the network with no security utilizing a standard TCP/IP protocol or the like. Alternatively, the sender may opt for a secure transmission mode, in which case the printer driver transmits the print job using a secure transmission protocol such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). These latter protocols provide a means for transmitting data across a network in encrypted format to prevent electronic interception of the data.

[0040] In the present invention, the print job is preferably transmitted using one of the aforementioned secure transmission protocols. As will be discussed in more detail below, utilization of a secure transmission protocol in the present invention is one method of providing an indication to the print node to distinguish a print job that requires authentication before printout from one that does not. However, the print job may also be transmitted utilizing a non-secure TCP/IP protocol, such as by providing a special driver at the sending node to encrypt the data before transmission and then transmitting the encrypted data to the print node. In such a case, the print node would first decrypt the encrypted print data before continuing to process the data according to the invention.

[0041] As seen in Figure 5, in step S501 the sender submits the print job along with unique identification information, sometimes called a distinguished name, identifying the person who is the intended recipient. This information is generally contained in a digital certificate. The identification information links the print job to the intended recipient, so that only the intended recipient is able to print the print job. More specifically, identification information such as the intended recipient's first name, last name, country, locality (city), organization, organization unit, or other information that is unique to him is linked to the print job.

[0042] This information may be obtained and linked to the print job by various methods. For example, the sender could insert a smart-card into a smart-card reader located at the sending node, such as smart-card reader 15 connected to computer 10 as seen in Figure 1. The smart-card could contain the recipient's unique identification information in digital form which is supplied to the computer through smart-card interface 265. Alternatively, the information may be obtained from a digital certificate, obtained via a Public Key Infrastructure, over the Internet, by e-mail or some other means. In this case, the information could be downloaded to computer 10 over the Internet to be subsequently submitted with the print job.

[0043] After obtaining the aforementioned unique identification information, the sender selects the desired transmission protocol from the print driver and submits the print job. As previously mentioned, in the present invention the preferred transmission protocol is a secure transmission protocol such as SSL. Because SSL is readily available to provide any necessary data encryption during the transmission process, the use of SSL eliminates the need for a special driver in the sending node to encrypt the data before transmission. Additionally, as will be discussed below, the use of SSL provides an indication used by the print node to indicate that the print job is one that should only be printed out upon proper authentication by the intended recipient.

[0044] After selecting the transmission protocol and obtaining the intended recipient information according to the foregoing, the sender submits the data to be printed and the sending node transmits the data via the secure transmission protocol (step S502).

[0045] The aforementioned data is then received by the print node (step S503) via the secure transmission protocol. In the present invention, the print node assumes that all data received via a secure transmission protocol, here SSL, is confidential and requires authentication before printout; and as a consequence the print job is encrypted and stored by the print node. With this feature, the print node does not ordinarily require a special driver to read header information that would otherwise be required in order for the print node to determine whether the print job is intended to be confidential. Rather, the print job is identified as confidential by the print node merely by the transmission protocol that the print data is received on.

[0046] Upon receiving the data, the print node then processes the print data and digital certificate to securely store the print data. In step S504, the print node generates a unique symmetric key utilizing a symmetric encryption algorithm. The print node encrypts the print data with the symmetric key in step S505, encrypts the symmetric key with the public key of the print node, and stores the encrypted print data, either locally or remotely. Although the present invention is

described as preferably utilizing a symmetric key, an asymmetric key, such as a public/private key pair, may also be utilized in the same manner as the symmetric key. It should also be noted that in a case where the print node is a printer, the print node uses the printer's public key to encrypt the symmetric key. However, in a case where the print node is a gateway to multiple printers, the print node uses the public key of the gateway to encyrpt the symmetric key. The reasons for this distinction will be described in more detail below.

[0047] Finally with regard to the print node encryption process of Figure 5, the print node submits print job identification information, the intended recipient identification information, storage location information for the stored encrypted print data, and the symmetric key encrypted (wrapped) with the printer's public key, to the print queue (step S506). The print node then waits for the intended recipient to arrive at the printer and present the proper authentication information in order to retrieve the print job and have it printed.

[0048] Figure 6 is a flowchart depicting the process whereby the aforementioned stored encrypted print data is printed out only in the presence of the intended recipient. In Figure 6, the print node is a printer itself rather than a gateway; a gateway arrangement is described below with regard to Figures 7A, 7B and 8.

[0049] As seen in Figure 6, the intended recipient presents authentication information to the printer to begin the printing process (step S601). This authentication process will now be described in more detail.

[0050] As briefly discussed above, in the present invention, a hard-copy printout submitted to a print node is not printed until the intended recipient arrives at the printer and is properly authenticated. The authentication process is generally initiated by the intended recipient presenting his unique identification information in digital form to the printer. For example, the intended recipient may insert a smart-card containing the aforementioned unique identification information identifying himself into a smart-card reader, such as smart-card reader 55.

[0051] Upon presenting the smart-card to the smart-card reader, the printer, such as printer 50, first verifies the integrity of the aforementioned unique identification information. The printer may then perform a "challenge/response" mechanism, or other process, to validate the identity of the recipient. If the recipient is authenticated (step S603), the printer then proceeds with the printout process. If the recipient is not authenticated, then notification is made of the authentication failure (step S604) by some means located at the printer. For example, the printer may contain a display device that presents a message to the recipient, or the printer itself may print out a sheet containing an error message.

[0052] Although the foregoing authentication process is described with regard to the use of smart-cards, other means of performing the authentication may also be employed. For example, the intended recipient could enter a PIN (Personal Identification Number) or a password from a keypad or touch display device located at the printer. The authentication may also be performed utilizing some other token reading device which contains the necessary information to permit the intended recipient to print out the image. Regardless of the means employed, so long as the proper authentication is provided by the intended recipient, the objectives of the present invention are achieved.

[0053] Once the intended recipient is authenticated, the printer then determines whether there are any print jobs queued for the intended recipient (step S605). In this process, the printer again utilizes the unique identification information of the intended recipient. The printer utilizes the information presented by the smart-card and compares it to the identification information stored in the print queue. If the printer determines that print jobs are queued for the intended recipient, the printout process continues. If however, the printer determines that no print jobs are queued for the intended recipient, then the recipient is notified that no print jobs are queued (step S606). Means similar to the above described means may be used for such notification.

[0054] After the printer determines that print jobs are queued for the intended recipient, the printer then retrieves the encrypted (wrapped) symmetric key and the print data storage location from the print queue (step S607). The printer then retrieves the encrypted print data (step S608) from the storage location for further processing.

[0055] Upon receiving the encrypted print data, the printer then decrypts (unwraps) the symmetric key obtained from the print queue using its private key (step S609), preferably via the printer's smart-chip, then utilizes this symmetric key to decrypt the encrypted print data (step S610). This process is performed by well known techniques contained in encryption/decryption logic 355 of printer 50.

[0056] Finally, the decrypted print data is utilized by the printer to output an image based on the print data using image printing techniques known in the art (step S611).

[0057] Next, the present invention will be discussed for a case where the print node is a gateway to one or multiple printers.

[0058] In the following discussion, the print node is preferably contained within a network server, such as server 40. Therefore, the print node and the printer, or other type of image forming device, are remote from one another. As a result, the printer and print node communicate with one another via a communication link. In the present invention, two types of communication links will be discussed. In Figures 7A and 7B, the communication link is assumed to be a secure transmission protocol such as SSL; in Figure 8, on the other hand, the communication link is assumed to be a standard TCP/IP protocol. As will become apparent in the following dis-

cussion, the process for transmitting data between the print node and the printer differs slightly depending on the type of communication link employed.

[0059] Figure 7A is a flowchart depicting substantially the same process as discussed with regard to Figure 6. However, some differences in the processing are present because the print node is a gateway rather than the printer itself.

[0060] In Figure 7A, steps S701 through S704 correspond to steps S601 through S604. Accordingly, the discussion of those steps applies equally with regard to Figure 7A and will not be repeated here.

[0061] After the printer authenticates the intended recipient (steps S702 and S703), the printer notifies the print node that the intended recipient has arrived at the printer (step S705).

[0062] Following notification by the printer that the intended recipient has arrived, the print node then performs the functions recited in steps S706 through S709 in the same manner as described with regard to steps S605 through S608 above. Namely, the print node determines whether any print jobs are queued for the intended recipient, obtains the encrypted symmetric key and storage location information, and retrieves the encrypted print data (step S709). At this point in the process, the next step taken by the print node differs depending on the type of communication link employed between the print node and the printer.

[0063] In Figure 7A, recall that a secure transmission protocol is employed. Because a secure protocol is used, it is assumed that the environment between the print node and the printer has sufficient security that transmitting the symmetric key in encrypted form from the print node to the printer is not necessary. Therefore, as shown in Figure 7A, once the print node retrieves the print data from the storage location, the print node uses its private key to decrypt the symmetric key and then transmits the encrypted print data and the symmetric key to the printer for processing by the printer (step S710).

[0064] Alternatively, as shown in Figure 7B, rather than transmitting the symmetric key and encrypted print data to the printer for processing, the print node may decrypt the symmetric key using its private key, then use the symmetric key to decrypt the print data itself and transmit the decrypted print data to the printer (steps S760 and S761). With this embodiment, the printer is not required to decrypt the print data, but merely prints out an image based on the decrypted print data received from the print node. This is the preferred embodiment since the print node generally has greater resources available to perform the required decryption processes than does the printer. Although this is a somewhat less secure transmission than that described above with regard to Figure 7A, the SSL protocol provides ample security for the data transmission between the print node and the printer, thereby achieving secure authorized printing of the image.

[0065] However, with reference to Figure 8, it is assumed that a standard TCP/IP protocol is utilized between the print node and the printer. In this case, an additional encryption process is desired to provide security of the data during the transmission process from the print node to the printer in order to prevent electronic interception. Accordingly, in step S810, the print node decrypts the encrypted symmetric key using its private key, then re-encrypts the symmetric key with the public key of the printer. In this manner, the symmetric key can only be decrypted by the private key of the destination printer. After encrypting the symmetric key with the printer's public key, the print node transmits the encrypted print data and the symmetric key encrypted with the printer's public key to the printer (step S811).

[0066] Referring again to Figure 7A, upon receiving the encrypted print data and the symmetric key from the print node, the printer then decrypts the print data utilizing the symmetric key and prints out an image based on the decrypted print data (steps S711 and S712) in the same manner as described with regard to steps S610 and S611.

[0067] Again referring to Figure 8, the processing by the printer after receiving the encrypted print data and encrypted symmetric key from the print node is slightly different than that described in Figure 7A due to the encryption of the symmetric key as described above. In Figure 8, upon receiving the encrypted print data and encrypted symmetric key, the printer utilizes its private key to decrypt the symmetric key (step S812). After decrypting the symmetric key, the printer then decrypts the print data and prints out an image based on the decrypted data (steps S813 and S814) in the same manner as described with regard to steps S610 and S611.

[0068] It will be appreciated that the invention extends to a signal conveying machine readable instructions for causing a print mode to operate as described above, as well as a computer readable medium storing such instructions. Such a signal may be downloaded from, for example, the Internet or a network.

[0069] The invention has been described with particular illustrative embodiments. It is to be understood that the invention is not limited to the above-described embodiments and that various changes and modifications may be made by those of ordinary skill in the art without departing from the spirit and scope of the invention.

Claims

1. A method for authorized printout of an image corresponding to print data received at a print node from a network, comprising:

   encrypting the print data by the print node and storing the encrypted print data without print-

out;

receiving authentication of an intended recipient to print the print data; and

decrypting the encrypted print data by the print node and printing the decrypted print data by an image forming device, responsive to receipt of authentication in said receiving step.

2. A method according to Claim 1, wherein the print data is encrypted by the print node utilizing a unique encrypting key.

3. A method according to Claim 2, wherein the unique encrypting key is a symmetric key randomly generated, utilized by a symmetric algorithm.

4. A method according to Claim 2, wherein the unique encrypting key is a public key of a public/private key pair being primarily in the sole possession of the print node, utilized by an asymmetric algorithm.

5. A method according to Claim 3, wherein the symmetric key is further encrypted using a public key of a public/private key pair being primarily in the sole possession of the print node.

6. A method according to Claim 5, wherein the encryption is performed by a smart-chip residing in the printer.

7. A method according to Claim 1, wherein the print node is the image forming device itself.

8. A method according to Claim 1, wherein the print node is a gateway to multiple image forming devices.

9. A method according to Claim 1, wherein the print data received by the print node is encrypted.

10. A method according to Claim 9 further comprising the step of decrypting the encrypted print data received by the print node before said encrypting step.

11. A method according to Claim 1, wherein the authentication is supplied at the image forming device.

12. A method according to Claim 1, wherein the authentication is supplied utilizing a smart-card reader connected to the print node and located at the image forming device.

13. A method according to Claim 1, wherein the print data received at the print node is identified as requiring user authentication in order to print the data by the fact it has been received over a secure transmission protocol.

14. An apparatus for authorized printout of an image corresponding to print data received at a print node from a network, the apparatus comprising:

a memory including a region for storing executable process steps and data for the image; and

a processor for executing the executable process steps;

wherein the executable process steps include (a) encrypting the print data by the print node and storing the encrypted print data without printout; (b) receiving authentication of an intended recipient to print the print data; and (c) decrypting the encrypted print data by the print node and printing the decrypted print data by an image forming device, responsive to receipt of authentication in said receiving step.

15. An apparatus according to Claim 14, wherein the print data is encrypted by the print node utilizing a unique encrypting key.

16. An apparatus according to Claim 15, wherein the unique encrypting key is a symmetric key randomly generated, utilized by a symmetric algorithm.

17. An apparatus according to Claim 15, wherein the unique encrypting key is a public key of a public/private key pair being primarily in the sole possession of the print node, utilized by an asymmetric algorithm.

18. An apparatus according to Claim 16, wherein the symmetric encrypting key is further encrypted using a public key of a public/private key pair being primarily in the sole possession of the print node.

19. An apparatus according to Claim 18, wherein the encryption is performed by a smart-chip residing in the printer.

20. An apparatus according to Claim 14, wherein the print node is the image forming device.

21. An apparatus according to Claim 14, wherein the print node is a gateway to multiple image forming devices.

22. An apparatus according to Claim 14, wherein the print data received by the print node is encrypted.

23. An apparatus according to Claim 22 further comprising the step of decrypting the encrypted print data received by the print node before said encrypting step.

24. An apparatus according to Claim 14, wherein the authorization is supplied at the image forming device.

25. An apparatus according to Claim 14, wherein the authentication is supplied utilizing a smart-card reader connected to the print node and located at the image forming device.

26. An apparatus according to Claim 14, wherein the print data received at the print node is identified as requiring user authentication in order to print the data by the fact it has been received over a secure transmission protocol.

27. A computer-readable medium which stores computer-executable process steps for authorized printout of an image corresponding to print data received at a print node from a network, the computer-executable process steps comprising:

encrypting the print data by the print node and storing the encrypted print data without printout;
receiving authentication of an intended recipient to print the print data; and
decrypting the encrypted print data by the print node and printing the decrypted print data by an image forming device, responsive to receipt of authentication in said receiving step.

28. A computer-readable medium according to Claim 27, wherein the print data is encrypted by the print node utilizing a unique encrypting key.

29. A computer-readable medium according to Claim 28, wherein the unique encrypting key is a symmetric key randomly generated, utilized by a symmetric algorithm.

30. A computer-readable medium according to Claim 28, wherein the unique encrypting key is a public key of a public/private key pair being primarily in the sole possession of the print node, utilized by an asymmetric algorithm.

31. A computer-readable medium according to Claim 29, wherein the symmetric encrypting key is further encrypted using a public key of a public/private key pair being primarily in the sole possession of the print node.

32. A computer-readable medium according to Claim 31, wherein the encryption is performed by a smart-chip residing in the printer.

33. A computer-readable medium according to Claim 27, wherein the print node is the image forming device.

34. A computer-readable medium according to Claim 27, wherein the print node is a gateway to multiple image forming devices.

35. A computer-readable medium according to Claim 27, wherein the print data received by the print node is encrypted.

36. A computer-readable medium according to Claim 35 further comprising the step of decrypting the encrypted print data received by the print node before said encrypting step.

37. A computer-readable medium according to Claim 27, wherein the authentication is supplied at the image forming device.

38. A computer-readable medium according to Claim 27, wherein the authentication is supplied utilizing a smart-card reader connected to the print node and located at the image forming device.

39. A computer-readable medium according to Claim 27, wherein the print data received at the print node is identified as requiring user authentication in order to print the data by the fact it has been received over a secure transmission protocol.

40. An image forming device for authorized printout of an image corresponding to print data received at a print node from a network, the image forming device comprising:

a receiver for receiving data;
an image generator for generating an image from image data;
a memory including a region for storing executable process steps; and
a processor for executing the executable process steps,
wherein the executable process steps include: (a) encrypting the print data by the print node and storing the encrypted print data without printout; (b) receiving authentication of an intended recipient to print the print data; and (c) decrypting the encrypted print data by the print node and printing the decrypted print data by the image forming device, responsive to receipt of authorization in said receiving step.

41. An image forming device according to Claim 40, wherein the print data is encrypted by the print node utilizing a unique encrypting key.

42. An image forming device according to Claim 41, wherein the unique encrypting key is a symmetric

key randomly generated, utilized by a symmetric algorithm.

43. An image forming device according to Claim 41, wherein the unique encrypting key is a public key of a public/private key pair being primarily in the sole possession of the print node, utilized by an asymmetric algorithm.

44. An image forming device according to Claim 42, wherein the symmetric encrypting key is further encrypted using a public key of a public/private key pair being primarily in the sole possession of the print node.

45. An image forming device according to Claim 44, wherein the encryption is performed by a smart-chip residing in the printer.

46. An image forming device according to Claim 40, wherein the print node is the image forming device.

47. An image forming device according to Claim 40, wherein the print node is a gateway to multiple image forming devices.

48. An image forming device according to Claim 40, wherein the print data received by the print node is encrypted.

49. An image forming device according to Claim 48 further comprising the step of decrypting the encrypted print data received by the print node before said encrypting step.

50. An image forming device according to Claim 40, wherein the authentication is supplied at the image forming device.

51. An image forming device according to Claim 40, wherein the authentication is supplied utilizing a smart-card reader connected to the print node and located at the image forming device.

52. An image forming device according to Claim 40, wherein the print data received at the print node is identified as requiring user authentication in order to print the data by the fact it has been received over a secure transmission protocol.

53. A signal conveying machine readable instructions for causing a processor to perform a method according to any one of claims 1 to 13 or for causing a computer to act as an apparatus according to any one of claims 14 to 26 or causing an interface device to act as a driver for an image generator for use in an image forming device according to any one of claims 40 to 52.

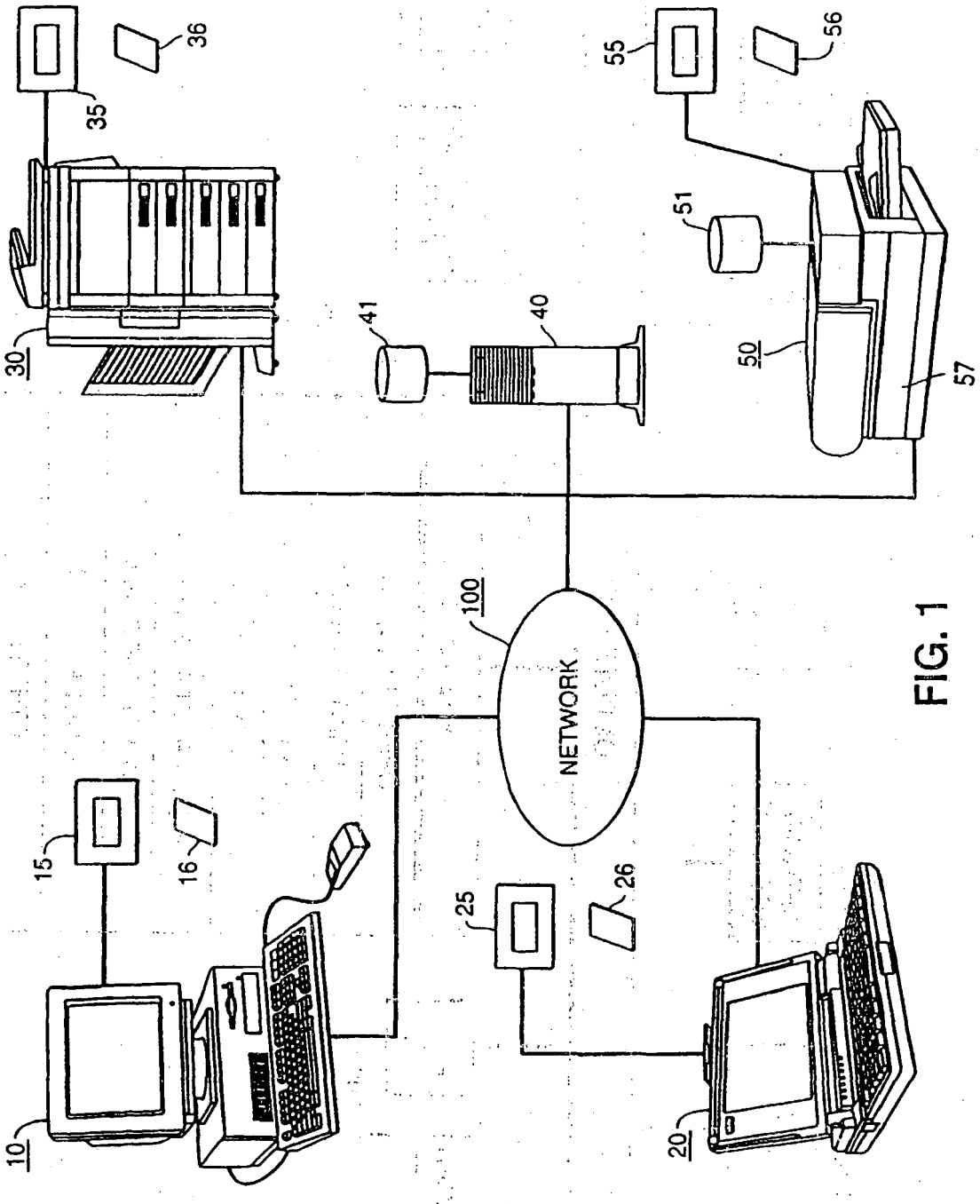

FIG. 1

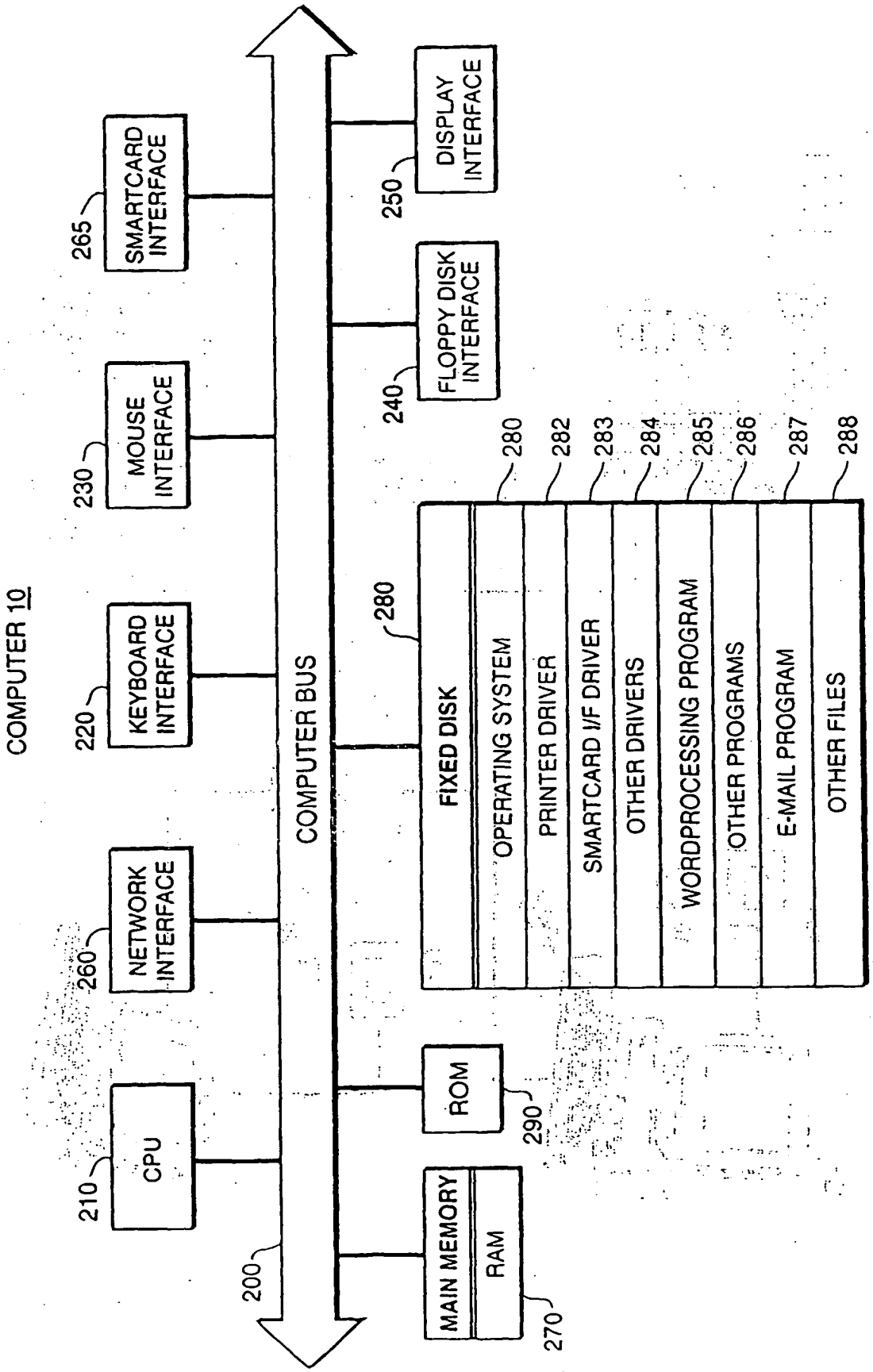
COMPUTER 10
COMPUTER BUS
200
CPU
210
NETWORK INTERFACE
260
KEYBOARD INTERFACE
220
MOUSE INTERFACE
230
SMARTCARD INTERFACE
265
DISPLAY INTERFACE
250
FLOPPY DISK INTERFACE
240
FIXED DISK
280
OPERATING SYSTEM
280
PRINTER DRIVER
282
SMARTCARD I/F DRIVER
283
OTHER DRIVERS
284
WORDPROCESSING PROGRAM
285
OTHER PROGRAMS
286
E-MAIL PROGRAM
287
OTHER FILES
288
ROM
290
MAIN MEMORY
RAM
270

FIG. 2

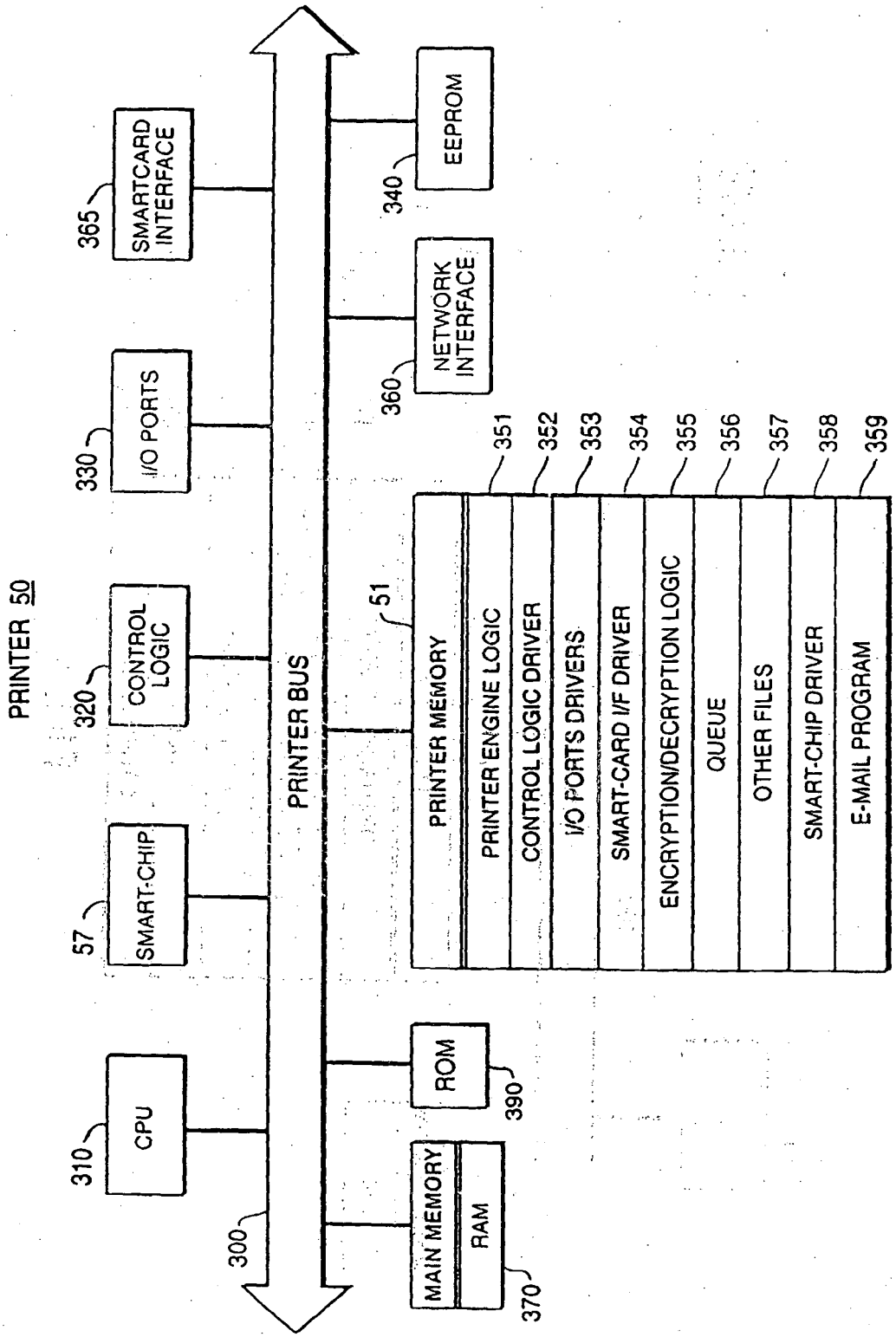
PRINTER 50
PRINTER BUS
300
310
CPU
57
SMART-CHIP
320
CONTROL LOGIC
330
I/O PORTS
365
SMARTCARD INTERFACE
MAIN MEMORY
RAM
370
ROM
390
51
PRINTER MEMORY
PRINTER ENGINE LOGIC
CONTROL LOGIC DRIVER
I/O PORTS DRIVERS
SMART-CARD I/F DRIVER
ENCRYPTION/DECRYPTION LOGIC
QUEUE
OTHER FILES
SMART-CHIP DRIVER
E-MAIL PROGRAM
351
352
353
354
355
356
357
358
359
360
NETWORK INTERFACE
340
EEPROM

FIG. 3

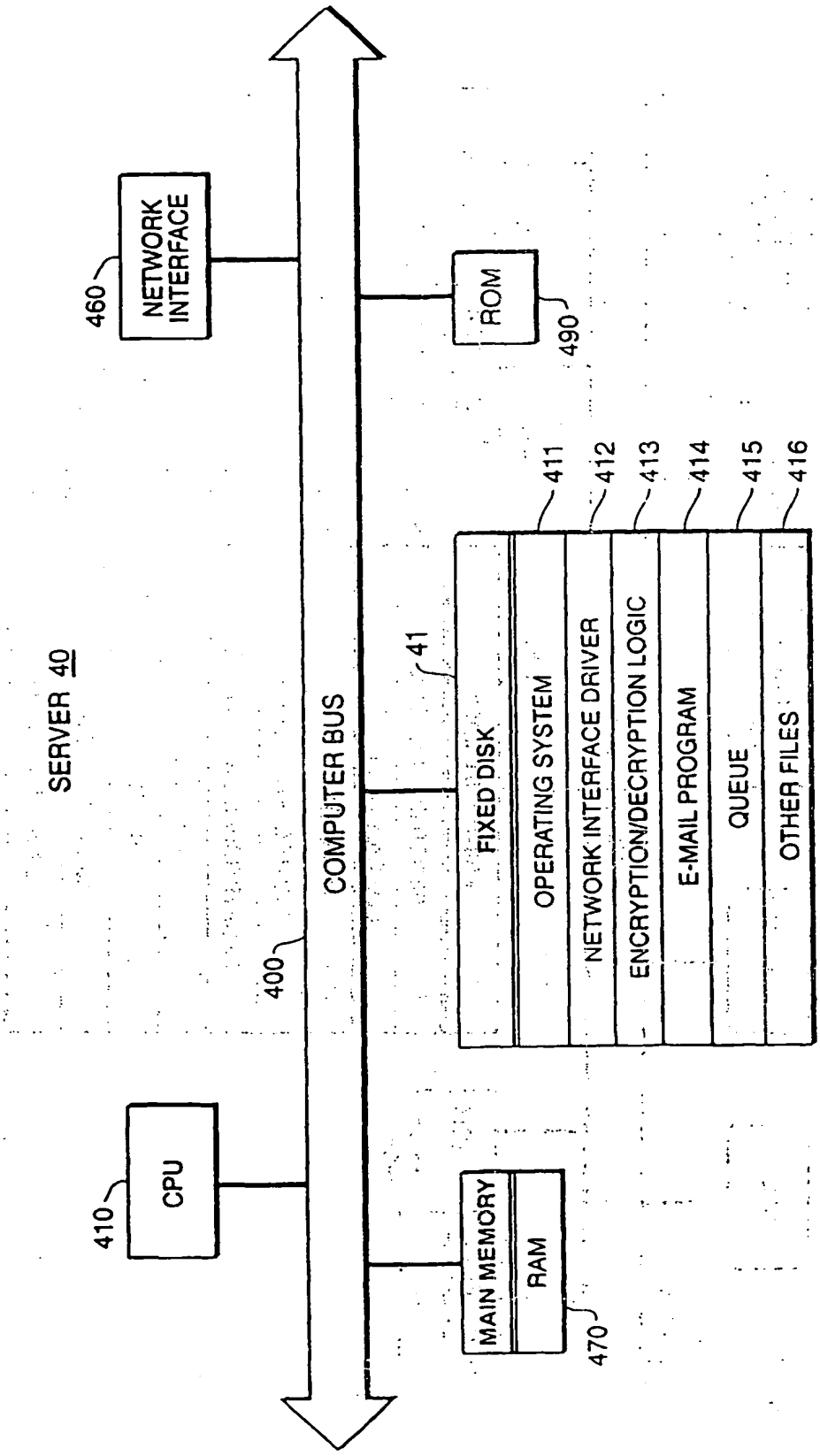
SERVER 40
NETWORK INTERFACE
460
ROM
490
COMPUTER BUS
400
41
FIXED DISK
OPERATING SYSTEM
NETWORK INTERFACE DRIVER
ENCRYPTION/DECRYPTION LOGIC
E-MAIL PROGRAM
QUEUE
OTHER FILES
411
412
413
414
415
416
CPU
410
MAIN MEMORY
RAM
470

FIG. 4

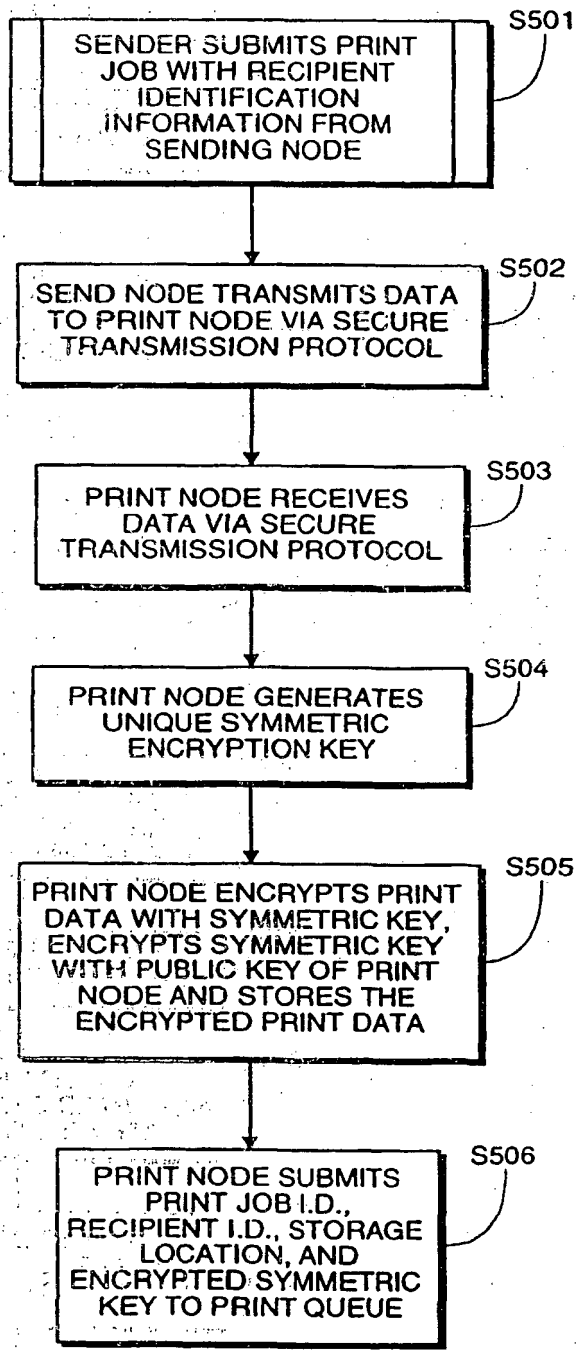
S501
SENDER SUBMITS PRINT JOB WITH RECIPIENT IDENTIFICATION INFORMATION FROM SENDING NODE
S502
SEND NODE TRANSMITS DATA TO PRINT NODE VIA SECURE TRANSMISSION PROTOCOL
S503
PRINT NODE RECEIVES DATA VIA SECURE TRANSMISSION PROTOCOL
S504
PRINT NODE GENERATES UNIQUE SYMMETRIC ENCRYPTION KEY
S505
PRINT NODE ENCRYPTS PRINT DATA WITH SYMMETRIC KEY, ENCRYPTS SYMMETRIC KEY WITH PUBLIC KEY OF PRINT NODE AND STORES THE ENCRYPTED PRINT DATA
S506
PRINT NODE SUBMITS PRINT JOB I.D., RECIPIENT I.D., STORAGE LOCATION, AND ENCRYPTED SYMMETRIC KEY TO PRINT QUEUE

FIG. 5

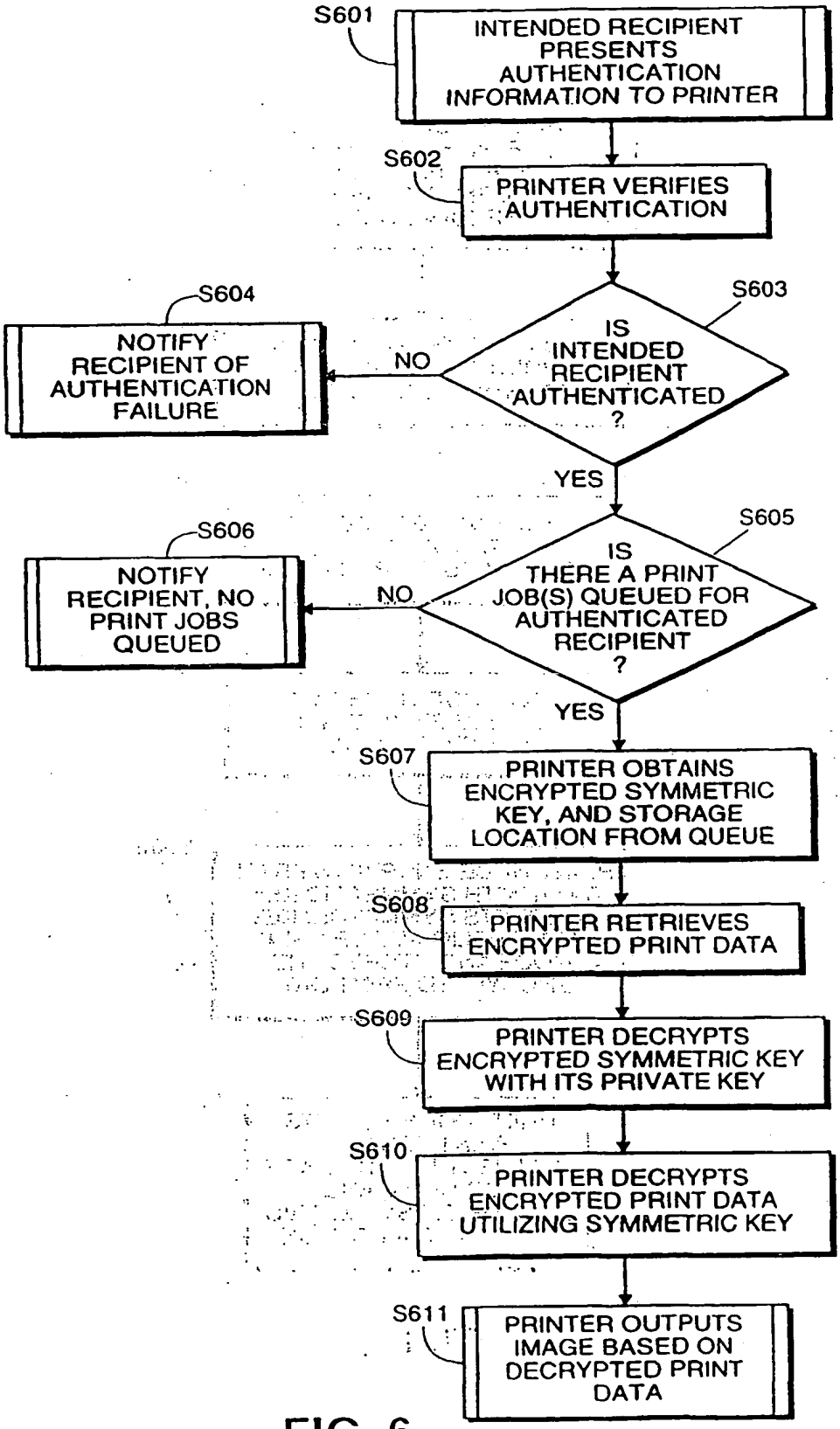
S601
INTENDED RECIPIENT PRESENTS AUTHENTICATION INFORMATION TO PRINTER
S602
PRINTER VERIFIES AUTHENTICATION
S603
IS INTENDED RECIPIENT AUTHENTICATED ?
NO
S604
NOTIFY RECIPIENT OF AUTHENTICATION FAILURE
YES
S605
IS THERE A PRINT JOB(S) QUEUED FOR AUTHENTICATED RECIPIENT ?
NO
S606
NOTIFY RECIPIENT, NO PRINT JOBS QUEUED
YES
S607
PRINTER OBTAINS ENCRYPTED SYMMETRIC KEY, AND STORAGE LOCATION FROM QUEUE
S608
PRINTER RETRIEVES ENCRYPTED PRINT DATA
S609
PRINTER DECRYPTS ENCRYPTED SYMMETRIC KEY WITH ITS PRIVATE KEY
S610
PRINTER DECRYPTS ENCRYPTED PRINT DATA UTILIZING SYMMETRIC KEY
S611
PRINTER OUTPUTS IMAGE BASED ON DECRYPTED PRINT DATA

FIG. 6

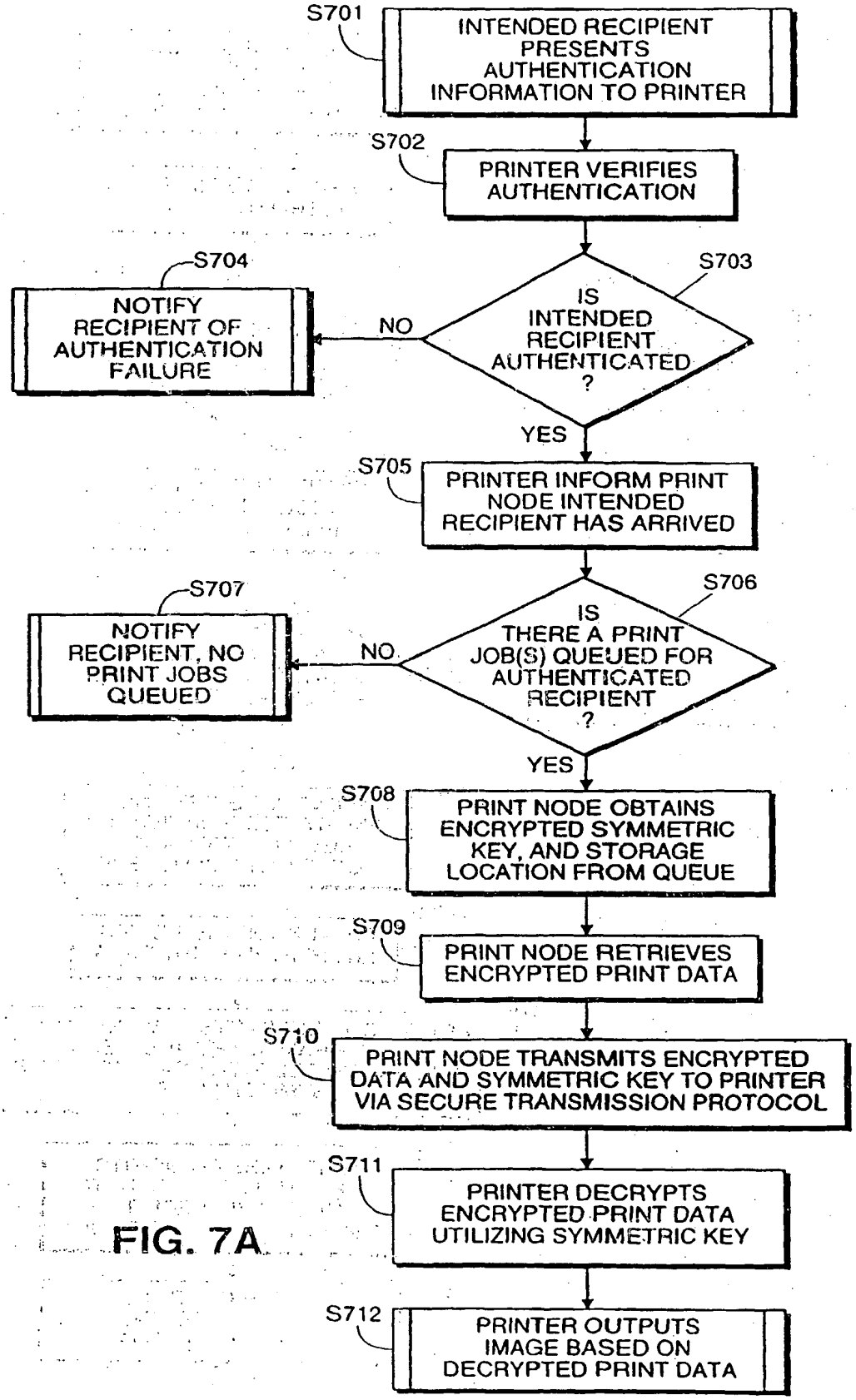
S701
INTENDED RECIPIENT PRESENTS AUTHENTICATION INFORMATION TO PRINTER
S702
PRINTER VERIFIES AUTHENTICATION
S703
IS INTENDED RECIPIENT AUTHENTICATED ?
NO
S704
NOTIFY RECIPIENT OF AUTHENTICATION FAILURE
YES
S705
PRINTER INFORM PRINT NODE INTENDED RECIPIENT HAS ARRIVED
S706
IS THERE A PRINT JOB(S) QUEUED FOR AUTHENTICATED RECIPIENT ?
NO
S707
NOTIFY RECIPIENT, NO PRINT JOBS QUEUED
YES
S708
PRINT NODE OBTAINS ENCRYPTED SYMMETRIC KEY, AND STORAGE LOCATION FROM QUEUE
S709
PRINT NODE RETRIEVES ENCRYPTED PRINT DATA
S710
PRINT NODE TRANSMITS ENCRYPTED DATA AND SYMMETRIC KEY TO PRINTER VIA SECURE TRANSMISSION PROTOCOL
S711
PRINTER DECRYPTS ENCRYPTED PRINT DATA UTILIZING SYMMETRIC KEY
S712
PRINTER OUTPUTS IMAGE BASED ON DECRYPTED PRINT DATA

FIG. 7A

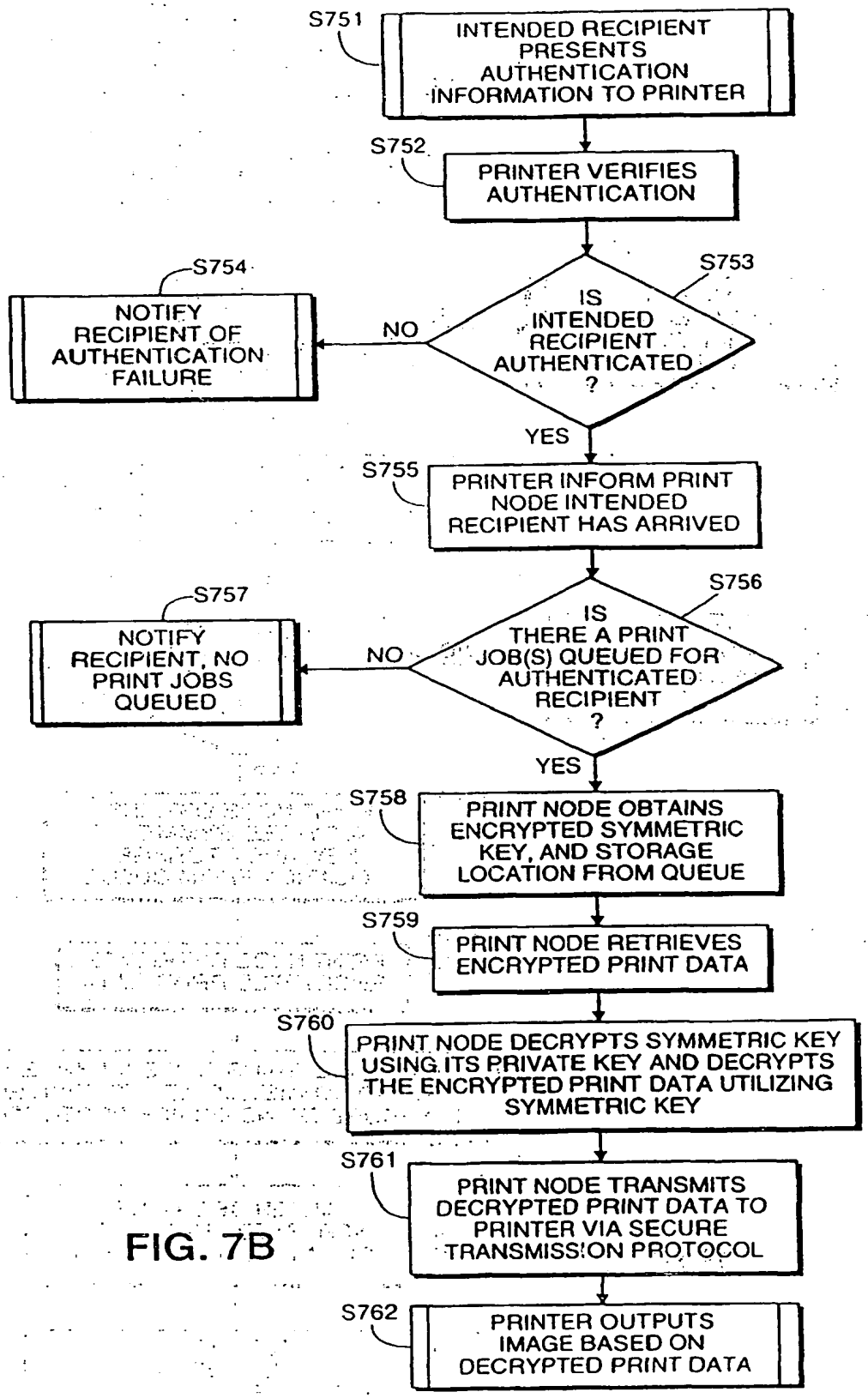
S751
INTENDED RECIPIENT PRESENTS AUTHENTICATION INFORMATION TO PRINTER
S752
PRINTER VERIFIES AUTHENTICATION
S753
IS INTENDED RECIPIENT AUTHENTICATED ?
NO
S754
NOTIFY RECIPIENT OF AUTHENTICATION FAILURE
YES
S755
PRINTER INFORM PRINT NODE INTENDED RECIPIENT HAS ARRIVED
S756
IS THERE A PRINT JOB(S) QUEUED FOR AUTHENTICATED RECIPIENT ?
NO
S757
NOTIFY RECIPIENT, NO PRINT JOBS QUEUED
YES
S758
PRINT NODE OBTAINS ENCRYPTED SYMMETRIC KEY, AND STORAGE LOCATION FROM QUEUE
S759
PRINT NODE RETRIEVES ENCRYPTED PRINT DATA
S760
PRINT NODE DECRYPTS SYMMETRIC KEY USING ITS PRIVATE KEY AND DECRYPTS THE ENCRYPTED PRINT DATA UTILIZING SYMMETRIC KEY
S761
PRINT NODE TRANSMITS DECRYPTED PRINT DATA TO PRINTER VIA SECURE TRANSMISSION PROTOCOL
S762
PRINTER OUTPUTS IMAGE BASED ON DECRYPTED PRINT DATA

FIG. 7B

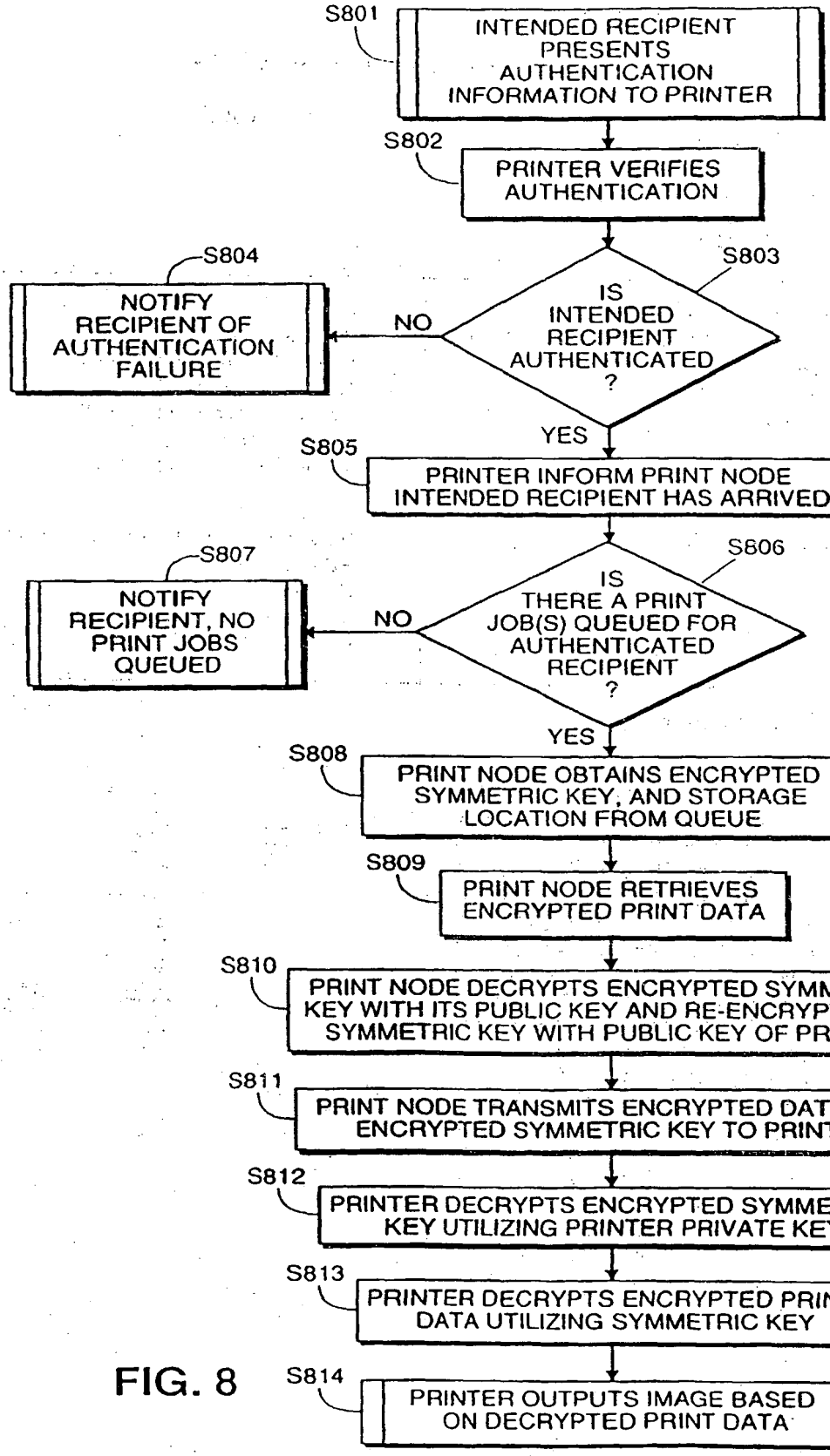
S801
INTENDED RECIPIENT PRESENTS AUTHENTICATION INFORMATION TO PRINTER
S802
PRINTER VERIFIES AUTHENTICATION
S803
IS INTENDED RECIPIENT AUTHENTICATED ?
NO
S804
NOTIFY RECIPIENT OF AUTHENTICATION FAILURE
YES
S805
PRINTER INFORM PRINT NODE INTENDED RECIPIENT HAS ARRIVED
S806
IS THERE A PRINT JOB(S) QUEUED FOR AUTHENTICATED RECIPIENT ?
NO
S807
NOTIFY RECIPIENT, NO PRINT JOBS QUEUED
YES
S808
PRINT NODE OBTAINS ENCRYPTED SYMMETRIC KEY, AND STORAGE LOCATION FROM QUEUE
S809
PRINT NODE RETRIEVES ENCRYPTED PRINT DATA
S810
PRINT NODE DECRYPTS ENCRYPTED SYMMETRIC KEY WITH ITS PUBLIC KEY AND RE-ENCRYPTS THE SYMMETRIC KEY WITH PUBLIC KEY OF PRINTER
S811
PRINT NODE TRANSMITS ENCRYPTED DATA AND ENCRYPTED SYMMETRIC KEY TO PRINTER
S812
PRINTER DECRYPTS ENCRYPTED SYMMETRIC KEY UTILIZING PRINTER PRIVATE KEY
S813
PRINTER DECRYPTS ENCRYPTED PRINT DATA UTILIZING SYMMETRIC KEY
S814
PRINTER OUTPUTS IMAGE BASED ON DECRYPTED PRINT DATA

FIG. 8